Prevalence of Sharing Access Credentials in Electronic Medical Records

Original Article

Healthc Inform Res. 2017 July;23(3):176-182.
https://doi.org/10.4258/hir.2017.23.3.176
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Prevalence of Sharing Access Credentials in Electronic Medical Records

Ayal Hassidim, MD[1]*, Tzfania Korach, MD[2]*, Rony Shreberk-Hassidim, MD[3], Elena Thomaidou, MD[3], Florina Uzefovsky, PhD[4], Shahar Ayal, PhD[5], Dan Ariely, PhD[6]

[1]Department of Plastic Surgery, Hadassah-Hebrew University Medical Center, Jerusalem, Israel; [2]Division of General Internal Medicine and Primary Care, Brigham and Women's Hospital, Harvard Medical School, Boston, MA, USA; [3]Department of Dermatology, Hadassah-Hebrew University Medical Center, Jerusalem, Israel; [4]Ben-Gurion University of the Negev, Be'er Sheva, Israel; [5]Interdisciplinary Center, Herzliya, Israel; [6]Duke University, Durham, NC, USA

Objectives: Confidentiality of health information is an important aspect of the physician patient relationship. The use of digital medical records has made data much more accessible. To prevent data leakage, many countries have created regulations regarding medical data accessibility. These regulations require a unique user ID for each medical staff member, and this must be protected by a password, which should be kept undisclosed by all means. **Methods:** We performed a four-question Google Forms-based survey of medical staff. In the survey, each participant was asked if he/she ever obtained the password of another medical staff member. Then, we asked how many times such an episode occurred and the reason for it. **Results:** A total of 299 surveys were gathered. The responses showed that 220 (73.6%) participants reported that they had obtained the password of another medical staff member. Only 171 (57.2%) estimated how many time it happened, with an average estimation of 4.75 episodes. All the residents that took part in the study (45, 15%) had obtained the password of another medical staff member, while only 57.5% (38/66) of the nurses reported this. **Conclusions:** The use of unique user IDs and passwords to defend the privacy of medical data is a common requirement in medical organizations. Unfortunately, the use of passwords is doomed because medical staff members share their passwords with one another. Strict regulations requiring each staff member to have it's a unique user ID might lead to password sharing and to a decrease in data safety.

Keywords: Electronic Medical Records, Personal Health Records, Confidentiality, Health Insurance Portability and Accountability Act, Medical Legislation

Submitted: December 26, 2016
Revised: May 7, 2017
Accepted: June 28, 2017

Corresponding Author
Ayal Hassidim, MD
Department of Plastic Surgery, Hadassah-Hebrew University Medical Center, Jerusalem 9112001, Israel. Tel: +972-2-6777111, E-mail: ayalha@gmail.com
*These two authors contributed equally to this work.

I. Introduction

"Whatever, in the course of my practice, I may see or hear (even when not invited), whatever I may happen to obtain knowledge of, if it be not proper to repeat it, I will keep sacred and secret within my own breast" [1]. Trust is one of the pillars of physician-patient interaction. For every patient to feel comfortable providing the exact and full details required for the medical care, he or she must trust the healthcare system's ability to keep this information confidential and must trust that it will be used only for the benefit of the patient [2]. With the widening adoption of Electronic Medical Records (EMRs) throughout healthcare organizations [3-5], patient

information finds its way far beyond the original situation in which it was revealed. The ease of access to information such computerized systems provide is a two-edged sword. The same mechanisms that enable healthcare providers to easily access any required piece of information with ease, can also be exploited for unjustified access competitors and insiders alike [5].

EMRs store extensive and highly sensitive information about patients, including personal, demographic, and financial information, making it a valuable target for attacks for various goals [5-7]. In addition to storage of personally-confidential information, healthcare organizations rely on computerized systems for a vast array of functions from setting appointments to critical life-supporting devices [8]. An attack on such computer systems can lead to extensive damage, from breaching the privacy of patients to disruption of healthcare operations and direct injury to patients.

The confidentiality of the patient's information is legally protected. In the United States, Title Two of the 'Health Insurance Portability and Accountability Act' (HIPAA) and subtitle D of the 'Health Information Technology for Economic and Clinical Health Act' impose requirements on healthcare organizations regarding the confidentiality of patients' information [9]. The legal basis of privacy requirements in Israel is the 'Privacy Protection Act' of 1981, which deals with sensitive personal information in general [10]. The Ministry of Health's Circular (MoHC) 18/12 from 2012 and the MoHC 3/15 from 2015 adapt the Privacy Protection Act's requirements to the healthcare setting. It relies on the 27799 ISO standard and requires the implementation of this standard [10,11].

In particular, organizations are required to predict and to ameliorate possible security risks through risk analysis and consequential risk management. The actual implementation of a security policy must be enforced by sanctions on workers violating their predefined permissions and rules. Following the general principle of limiting the exposure of protected health information (PHI) to the minimum necessary, the above-mentioned regulations require a clear definition of each worker's role and access privileges. This means that there is a need to authenticate the identity of each worker, control his/her access to relevant data, and audit any editing of data, including accesses for retrieval only, of PHI [9-11].

Based on reports from the last 6 years, the confidentiality of 135 million electronic patient records were breached in the United States alone [12]. While such events may evoke the image of sophisticated computer experts cracking the computer systems, many of these breaches were the results of organizations' own actions: losing a hard drive containing PHI in the Kaiser Permanente Anaheim [13]; accidental attachment of a confidential file to a 200-recipient email in the DENT Neurologic Institute [14], and deliberate revelation of confidential information by a former employee who manually photographed personal information in a Florida Digestive Health Specialists center [15]. These incidents demonstrate that, despite their sophistication, the security of such digital systems is still vulnerable to human actions, both innocent errors and malicious acts.

As demonstrated by these security incidents, the success of any regulation or technical security mechanism eventually depends on the actions of an organization's personnel and their cooperation. The inherent trade-off between the security and usability of a system may drive users to break security regulations and circumvent security measures in an honest attempt to fulfill their duties [5].

Apart from the large-scale mistakes and malicious acts described above, one of the most common breaches of PHI is the use of another's credentials to access patient information, i.e., the use of the EMR password of one medical staff member by another. As explained before, this kind of act is both unethical and dangerous. However, the extent of this practice has not been previously assessed. We have tried to determine the scale of this violation by conducting an Internet-based, open survey to assess the prevalence of access credentials (AC) sharing among medical and para-medical staff members.

II. Methods

1. Participants

We conducted a four-question Google Forms-based survey of medical and para-medical personal. We distributed the survey questionnaire to healthcare personnel we work with. In addition, we administered the survey through Facebook to members of groups that host discussions among medical and paramedical personnel. The survey was published on Facebook between January 8, 2014 to January 4, 2015, and it was open to responses from January 8, 2014 to January 5, 2015.

Based on the number of people who were directly emailed the link for the survey and the number of people who were exposed to it on their Facebook walls, the number of medical and paramedical personnel exposed to the survey was estimated to be about 2,500 people. Of those, a total of 300 pressed the link to start the survey, and 299 responded to the first question.

2. Measures

Since a direct question such as "Have you ever shared your AC with another staff member?" may suggest guilt and therefore lead to lower compliance rates and a recall bias, a less intimidating style was preferred, such as "Has anyone ever shared his/her AC with you?"

The survey was conducted in Hebrew, and was based on closed questions. A full translation of the survey questionnaire in English is shown in Figure 1, and it can be accessed online [16].

This study was granted an Institutional Review Board waiver by the Israeli Defense Force IRB, as no clinical personal subject data were collected or used.

Statistical analysis was performed using SPSS ver. 20 (IBM, Armonk, NY, USA).

III. Results

The main study objective was to determine the prevalence of AC sharing. Out of all the potential participants, 300 started the survey, 299 answered the first question, and they became the study cohort. Of these, 220 participants (73.6%) answered that they have been given the AC of at least one other medical or para-medical staff member. When asked how many ACs they had been given, only 171 (57.2%) responded with an average answer of 4.75 (min = 1, max = 25) ACs given to each user, for a total of 814 AC. Forty-nine (16.4%) people answered that they had been given the AC of another user but did not specify how many times. Thus, the main aim of the study was achieved. Other analysis was done to try and understand the reasons for this prevalence.

According to their opinions, when they were asked why they had been given the ACs of others and what their role was when they received them, their answers were divided as shown in Figures 2 and 3.

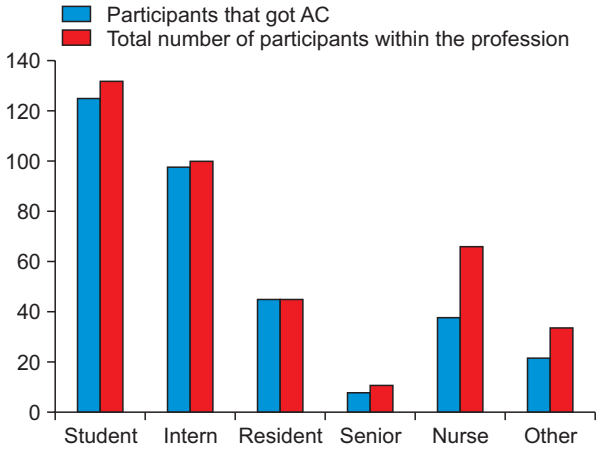

Figure 2. The percentage of participants that were given an access credentials (AC) out of the total number of participants with the same profession.

Health information security survey
We would like to learn about the suitability of the permissions given to medical personnel to their actual practice requirements. We will be grateful if you could contribute several moments to answer this questionnaire.
The survey is completely anonymous and the answers will be used solely for research purposes
1. Have you ever been given the authentication (log-in) credentials (e.g. username, password, magnetic card etc.) to the computer account of another worker
Yes / No
2. To how many accounts have you received log-in credentials?
If the exact number is unknown, please enter an estimate:
Why did you need the credentials for another worker's account?
a. The worker wanted to perform actions while away
b. Technical malfunction preventing me from using my own account
c. A limitation of the computer system forcing me to use the other worker's account in order to fulfill my duties
d. I was not given a user account despite having to use the system in order to fulfill my duties
e. The permissions granted to me did not allow me to fulfill my duties
f. Other:
3. What was your job title at the times of these incidents (or lack-thereof)?
More than one question are applicable
a. Student
b. Intern (PGY-1)
c. Resident\registrar
d. Non-consultant physician
e. Nursing staff
f. Consultant (senior) physician
g. Junior administrative staff
h. Senior administrative staff
i. Paramedic\emergency medical technician
j. Para-medical staff
k. Dentist
l. Dental technician
m. Combat medic

Figure 1. The complete, translated survey.

https://doi.org/10.4258/hir.2017.23.3.176

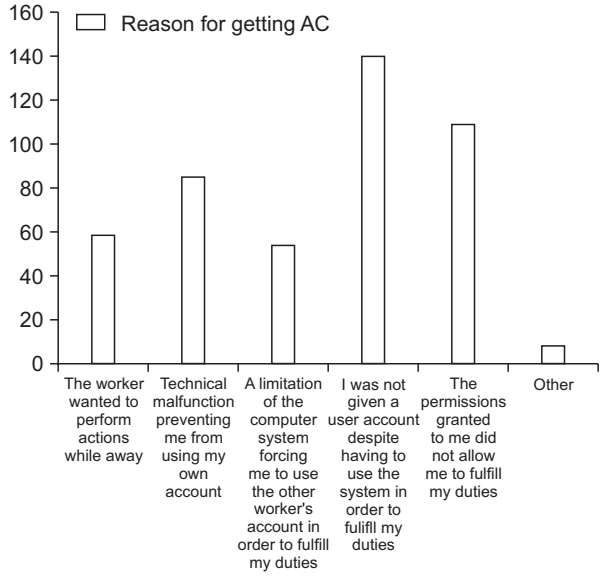

Figure 3. The number of participants that answered that they think they were given an access credentials (AC) for each reason.

An analysis of the reasons why participants needed the ACs of other staff members and the subgroups of diverse roles they held when they were given the ACs of other staff members was done. The reason "I was not given a user account despite having to use the system to fulfill my duties" was significantly more common among students than among non-student (working) staff members (0.77 ± 0.42 and 0.28 ± 0.45, respectively; $t_{(274)} = 9.44$, $p < 0.000$). Similar results were found for the reason "The permissions granted to me did not allow me to fulfill my duties", comparing students and non-student staff members (0.56 ± 0.49 vs. 0.25 ± 0.43; $t_{(272)} = 5.44$, $p < 0.001$).

When examining the intern group and analyzing the reason "I was not given a user account despite having to use the system to fulfill my duties" between the intern subgroup versus all other study participants, we found the following significant difference: interns (0.83 ± 0.37) and all other study participants (0.33 ± 0.47) conditions ($t_{(277)} = 9.08$, $p < 0.000$). When analyzing the reason "The permissions granted to me did not allow me to fulfill my duties" between the intern subgroup and all other study participants we found the following significant difference: interns (0.69 ± 0.46) and all other study participants (0.24 ± 0.42) conditions ($t_{(276)} = 8.04$, $p < 0.000$).

On the other hand, when examining the nurses group and analyzing the reason "I was not given a user account despite having to use the system to fulfill my duties" between the nurses subgroup and all other study participants, we found the following significant difference: nurses (0.1 ± 0.3) and

Table 1. Distribution of the mentioned reason for getting access credentials (AC) for each profession

	Total of participants with job title	Got AC	The worker wanted to perform actions while away	Technical malfunction preventing me from using my own account	A limitation of the computer system forcing me to use the other worker's account in order to fulfill my duties	I was not given a user account despite having to use the system fulfill my duties	The permissions granted to me did not allow me to fulfill my duties	Other
Student	132	125	25	44	27	96	67	4
Intern	100	98	25	43	27	79	64	0
Resident	45	45	14	27	14	30	27	0
Senior	11	8	2	7	2	7	5	0
Nurse	66	38	8	16	12	6	9	3
Other	34	22	12	11	5	11	10	1

all other study participants (0.61 ± 0.49) conditions ($t_{(278)}$ = –7.53, $p < 0.000$). When analyzing the reason "The permissions granted to me did not allow me to fulfill my duties" between the nurses subgroup and all other participants, we found the following significant difference: nurses (0.15 ± 0.36) and all other study participants (0.45 ± 0.5) conditions ($t_{(277)} = -4.38$, $p < 0.000$).

To counter the potential bias of one participant who obtained a large number of ACs as an intern, but also was given one AC as a senior, we decided to analyze the data of those who answered that they have been given an AC and who marked only one job title in the last question of the survey (e.g., student, intern, resident, and so on). We found that 152 of the recipients had only one profession. Of this cohort, 110 (72%) had been given at least one AC for a total of 338 AC obtained with an average of 4 ACs obtained per recipient. Students, interns, and residents (each group by itself) were given statistically significantly more ACs than the general population (p-values are 0.001, 0.008, and 0.001, respectively); nurses, on the contrary, received statistically significantly fewer ACs than the general population ($p < 0.001$), and senior physicians and the other group showed non-statistically significant results. Those results are compatible with the results we obtained in our first analysis. The details are presented in Table 1.

IV. Discussion

Protection of PHI confidentiality is a major concern for governments and commercial organizations alike, as demonstrated by laws and standards concerning this subject, such as HIPAA and ISO Standard 27799. In contrast to the Swiss-cheese safety system model [17], the strength of an information security system is determined by the strength of the weakest link and not by the strength of the whole system [18]. As past events show, even a single breach may render an information security system ineffective [14-16].

Medical staff must provide timely and efficient care while maintaining patient confidentiality. This may put medical staff members in a conflict between their duty and their obligation to meet security regulations. This conflict may be worsened by several practices. On the one hand, there is a frequent turn-over of junior staff between organizations and departments, up to every week in Israeli medical schools for students in their clinical rotations. On the other hand, the registration process is strict and lengthy. This combination may lead to a gap between the commencement of actual work and the granting of an AC allowing the new employee to have access to computerized systems. Furthermore, this may force these new employees and students to use other employee's credentials to fulfill their duties, explaining the higher frequency of this reason among students and interns.

Under-staffing, especially during on-call hours, may lead to the delegation of administrative tasks to para-medical and junior staff (such as interns and students). This creates a de facto need for them to be granted privileges that have not been granted to them in their original roles, and this could explain the higher frequency of the reason ("The permissions granted to me did not allow me to fulfill my duties") among students and interns for receiving the ACs of other staff members.

Another group of limited clinical privileges, nurses, actually demonstrated an opposite trend. Nurses reported that they were given fewer ACs compared to the general study population. Despite the similarity in the limitation of clinical privileges, this contrast may be explained by a very fundamental difference between the privileges and work of junior physicians and nurses. Regulations grant physicians a global and general privilege to perform any medical activity; while nurses are limited to only those activities specifically approved to be performed by nurses. This may enable a more precise definition of clinical duties, facilitating the matching of granted EMR privileges to the defined duties. Moreover, in unplanned clinical scenarios, the limited list of nurses' clinical privileges may prohibit them from performing the action in question and spares them the conflict between providing necessary care and following regulations. Nurses generally work under the guidance of a more privileged clinician (e.g., a physician) to whom they may transfer a duty outside of their permitted scope. A physician, as the clinical practitioner in charge, may be left with no option but to transfer an unplanned duty. This situation can become more relevant during on-call hours when interns and residents may be encountered with unexpected duties that require them to manipulate the use of EMR ACs to complete their tasks.

In the face of such security breaches, organizations may be tempted to strengthen the authentication process, for example, by requiring smart-cards and biometric authentication (multi-factor authentication). While having their merits, these measures can actually worsen the situation and drive users to further violate security regulations: physical tokens may be left for other users just like passwords, and biometric authentication may drive the users to completely avoid the electronic system and rely on paper forms, which could make EMR systems redundant. This may lead to deterioration of treatment because, when paper forms are used in an

 https://doi.org/10.4258/hir.2017.23.3.176

EMR-based environment, data can be lost or misplaced, and this can create risks for patients.

Our results show that current permission granting and authentication processes might cause more harm than good. In an attempt to achieve better security, usability is hindered to the level the users feel that the right thing to do is to violate the security regulations altogether. While the ISO standard on information security (ISO/IEC 27700) bases information security on the three principles of confidentiality, integrity and availability [19], it may be beneficial to keep in mind a fourth principle, usability, which is essential for end-user compliance and cooperation. Accordingly, when deciding on the privileges and authentication of users, an organization first has to take into consideration its own expectations from its employees and the level of flexibility and discretion each user needs and can handle.

As has been shown previously [20], reduction of ethical standards is a contagious behavior. As medical personnel, we know that sharing PHI is part of medical treatment, mainly when consultant help is required. We are afraid that, while residents share both legitimate information to give the best care to their patients and their ACs to fulfill their duties, there is an increased chance that they will feel free to share more information about their patients that is not simply related to their medical treatment [21].

The current survey was conducted using an anonymous, on-line platform. This administration method is advantageous to foster a sense of anonymity in responders, which allows them to reveal information that might otherwise be left concealed. The mere action of transferring an AC is considered a violation of security regulations, sometimes to the level of a felony. Any organization inquiring into such incidents may find itself legally liable for the actions of its employees. The employees themselves, on the other hand, may find themselves liable for either the incident itself or for the failure to report it, a violation on its own. However, as it was an anonymous survey, we were unable to link the reported reasons for AC breach to responders' professional phase, thus possibly mixing reasons relevant to different phases.

There were several limitations to this study. A question arises about the efficacy of an online questionnaire as a scientific tool. This question has been discussed by others, and the questionnaires considered were found as good as other, more customary, surveys [22]. The current participants were Hebrew-speaking medical personal who agreed to answer an Internet-based survey and might have had a prior interest in PHI, which could limit the generalizability of the findings. Another limitation is that the survey did not account for the professional stage at which the AC violations occurred. For instance, a senior physician may have answered that he/she was given an AC, but this may have happened when he/she was an intern, when there was less awareness of the importance of PHI.

The current findings emphasize that increased awareness of this issue is needed to improve EMR systems and the security of PHI. To our knowledge this is the first time questions like this were assessed in an academic manner, and the results support the hypothesis that AC sharing is a common practice in the medical world.

We call for two main recommendations. First, usability should be added as the fourth principal in planning EMRs and other PHI-containing medical records. Second, an additional option should be included for each EMR role that will grant it maximal privileges for one action. When this option is invoked, the senior physician/the PHI security officer would be informed. This would allow junior staff to perform urgent, lifesaving, decisions, without outwitting the EMR, and under formal retrospective supervision by the senior members in charge.

The next phase of this research will be a survey of medical staff when several declarations will be evaluated by the survey recipients (such as "I am not allowed to share my AC." - right/wrong). Then, episodes that describe AC sharing will be introduced to the survey recipients, and they will need to say whether AC sharing was the "right" thing to do in those scenarios. After that, they will have an open space to express other options to overcome the problem that was illustrated by each scenario. This should show the ambivalence that we all share as medical staff—we know we should not share ACs, but we still do so.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

References

1. Aghadiuno M. Hippocrates appraises 21st century doctors. Br J Gen Pract 2003;53(497):984-5.
2. Dorr Goold S, Lipkin M Jr. The doctor-patient relationship: challenges, opportunities, and strategies. J Gen Intern Med 1999;14 Suppl 1:S26-33.
3. Hesse BW, Hansen D, Finholt T, Munson S, Kellogg W, Thomas JC. Social participation in Health 2.0. Computer (Long Beach Calif) 2010;43(11):45-52.

4. Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. Proceedings of the 2009 ACM Workshop on Cloud Computing Security; 2009 Nov 13; Chicago, IL. p. 103-14.
5. Fernandez-Aleman JL, Senor IC, Lozoya Pao, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inform 2013;46(3): 541-62.
6. Zurita L, Nohr C. Patient opinion: EHR assessment from the users perspective. Stud Health Technol Inform 2004;107(Pt 2):1333-6.
7. Chhanabhai P, Holt A. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. MedGenMed 2007;9(1):8.
8. Strickland JH Jr, Hasson JH. A computer-controlled ventilator weaning system: a clinical trial. Chest 1993; 103(4):1220-6.
9. US Department of Health & Human Services. The HIPAA Privacy Rule [Internet]. Washington (DC): US Department of Health & Human Services; c2016 [cited at 2017 Jul 1]. Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/.
10. Afek A. Protecting information in health related computer systems. Jerusalem: Israel Ministry of Health, 2015.
11. Response of the Ministry of Health CEO Circular - Protection of Information in Computerized Systems in the Health System - Circular 9/12 [Internet]. Jerusalem: Ministry of Health Israel; 2012 [cited at 2017 Jul 1]. Available from: http://www.health.gov.il/hozer/mk18_2012.pdf.
12. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Washington (DC): US Department of Health and Human Services Office for Civil Rights; c2016 [cited at 2017 Jul 1]. Available from: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.
13. Lost flash drive at core of Kaiser Permanente Data Breach [Internet]. [place unknown]: CRN.com; c2013 [cited at 2017 Jul 1]. http://www.crn.com/news/security/240164674/lost-flash-drive-at-core-of-kaiser-permanente-data-breach.htm.
14. Watson ST, Miller M. Mass email by Dent Neurologic inadvertently breaches privacy of 10,200 patients [Internet]. Buffalo (NY): The Buffalo News; c2013 [cited at 2017 Jul 1]. Available from: http://buffalonews.com/2013/05/14/mass-email-by-dent-neurologic-inadvertently-breaches-privacy-of-10200-patients/.
15. Salman J. Patient data may have been leaked, doctors group warns [Internet]. Sarasota (FL): Herald-Tribune; c2013 [cited at 2017 Jul 1]. http://www.heraldtribune.com/news/20131125/patient-data-may-have-been-leaked-doctors-group-warns.
16. Hassidim A. Health information security survey. [place unknown: publisher unknown]; 2014.
17. Reason J. Human error: models and management. BMJ 2000;320(7237):768-70.
18. Flink CW. Weakest link in information system security. Proceedings of the Workshop for Application of Engineering Principles to System Security Design (WAEPSSD); 2002 Nov 6-8; Boston, MA.
19. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Muller G. Aspects of privacy for electronic health records. Int J Med Inform 2011;80(2):e26-31.
20. Gino F, Ayal S and Ariely D. Contagion and differentiation in unethical behavior the effect of one bad apple on the barrel. Psychol Sci 2009;20(3):393-8.
21. Welsh DT, Ordóñez LD, Snyder DG, Christian MS. The slippery slope: how small ethical transgressions pave the way for larger future transgressions. J Appl Psychol 2015;100(1):114-27.
22. Buhrmester M, Kwang T, Gosling SD. Amazon's Mechanical Turk: a new source of inexpensive, yet high-quality, data? Perspect Psychol Sci 2011;6(1):3-5.

 https://doi.org/10.4258/hir.2017.23.3.176